

REMARKS

Claims 12, 14-16 and 18-43 are pending in the present application. In the above amendments, claims 12, 16 and 20-22 have been amended, and new claims 34-43 have been added.

Applicant respectfully responds to this Office Action.

Claim Rejections – 35 USC § 103

The Examiner rejected claims 12, 14-16 and 18-33 under 35 U.S.C. §103(a) as being allegedly unpatentable over Dierks et al., The TLS Protocol, Version 1.0 (the Dierks publication) in view of U.S. Patent No. 7,237,261 to Huber et al. (the Huber patent), and further in view of U.S. Patent No. 6,955,299 to Pathmasuntharan et al. (the Pathmasuntharan patent).

The rejection of claim 12 as being unpatentable over the Dierks publication in view of the Huber patent and further in view of the Pathmasuntharan patent, is respectfully traversed. Claim 12, as amended, recites a “method for fast generation of a cryptographic key, comprising: generating a first public key for encrypting a first wireless communication; and generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.” Support for the amendment to claim 12 is in the original specification in paragraphs [0021] through [0022], and in Figure 2, steps 202-204. The Dierks publication fails to disclose or suggest, “generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key,” as recited in claim 12, and the Huber patent fails to remedy the disclosure deficiencies of the Dierks publication. The newly cited Pathmasuntharan patent discloses generating a transaction key, and communicates the generated transaction key to an enabler device before terminating a communication with the enabler device. See, column 13, lines 39-49, and Figure 8, reference points 6 and 7. Thus, the Pathmasuntharan patent teaches generating a transaction key before termination of a communication with the enabler device. Further, the transaction key is merely a random number which is stored by a smart card and an enabler device for comparison at the next transaction.

See, column 9, lines 7-12, column 11, lines 10-40, and column 12, lines 2-6. Applicants assert there is no disclosure or suggestion that the transaction key of the Pathmasuntharan patent is used for encrypting a second wireless communication. Therefore, since the Dierks publication, the Huber patent, and the Pathmasuntharan patent, do not disclose or suggest all of the recited features, Applicants respectfully request the Examiner to withdraw the rejection of claim 12.

It is respectfully submitted that dependent claims 14-15 and 32 are at least allowable for the reasons given above in relation to independent claim 12.

Claims 16-31 and 33 are wireless communication device, processor, and computer program product claims having features defined by language similar to that of method claims 12, 14-15 and 32. It is respectfully submitted that claims 16-31 and 33 are at least allowable for the reasons given above in relation to claims 12, 14-15 and 32.

New Claims

Support for new claims 34-43 may be located in the original specification at paragraphs [0019] – [0024]. Applicants respectfully asserts that new claims 34-43 recite patentable matter as discussed above with respect to claims 12-33, and for recitation of first and second private keys and first and second shared keys.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **August 4, 2008**

**By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295**

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502